Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

1. (Currently amended) A method of authenticating communication between a first and a second party, the method comprising:

determining whether a shared secret exists between a peer and a server;

establishing a first secure tunnel between the peer and the server using asymmetric encryption responsive to determining [[a]]the shared secret does not exist between the peer and the server;

receiving the shared secret via the first secure tunnel between the peer and the server responsive to the determining that [[a]]the shared secret does not exist between the peer and the server and to the establishing the first secure tunnel;

tearing down the first secure tunnel;

establishing a subsequent[[,]] new secure tunnel between the peer and the server using symmetric encryption and the shared secret after the tearing down the first secure tunnel and after the peer has received the shared secret;

mutually deriving a tunnel key for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent[[,]] new secure tunnel;

authenticating a relationship between the peer and the server within the subsequent new secure tunnel upon mutually deriving the tunnel key for the subsequent[[,]] new secure tunnel; and

cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel.

2. (Original) The method set forth in claim 1 further comprising the step of protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user.

Claims 3- 4 (Canceled)

5. (Previously Presented) The method set forth in claim 1 wherein the shared secret is a protected access credential (PAC).

6. (Original) The method set forth in claim 5 wherein the protected access credential includes a protected access credential key.

7. (Original) The method set forth in claim 6 wherein the protected access credential key is a strong entropy key.

8. (Original) The method set forth in claim 7 wherein the entropy key is a 32-octet key.

9. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential opaque element.

10. (Original) The method set forth in claim 6 wherein the protected access credential includes a protected access credential information element.

Claims 11 - 14 (Cancelled)

15. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using EAP-GTC.

16. (Original) The method set forth in claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

17. (Currently amended) A system for communicating via a network, the system comprising:

means for providing a communication link between a peer and a server;

means for determining whether a shared secret exists between the peer and the server;

means for provisioning a shared secret between the peer and the server responsive to the means for determining whether the shared secret exists determining the shared secret does not exist, wherein the means for provisioning comprises means for establishing a first secure tunnel between the peer and server using asymmetric encryption, means for acquiring the shared secret through the first secure tunnel, and means for tearing down the first secure tunnel after the means for acquiring has acquired the shared secret;

means for establishing a subsequent[[,]] new secure tunnel utilizing the shared secret after the means for tearing down has torn down the first secure tunnel and responsive to the means for determining whether a shared secret exists determining that the shared secret exists, wherein the means for establishing the subsequent[[,]] new secure tunnel comprises means for deriving a tunnel key using symmetric cryptography based on the shared secret;

means for authenticating a relationship between the peer and the server within the subsequent[[,]] new secure tunnel; and

means for cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel.

18. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wireless network.

19. (Original) The system for communicating set forth in claim 17 wherein the communication link is a wired network.

20. (Original) The system for communicating set forth in claim 17 wherein the shared secret is a protected access credential (PAC).

21. (Original) The system for communicating set forth in claim 18 wherein the wireless network is an 802.11 wireless network.

Claims 22 -23 (Canceled)

24. (Currently amended) A wireless device, comprising:

a wireless network adapter for sending and receiving wireless signals with a server;

wherein the wireless device is configured to determine whether a shared secret exists between the wireless device and the server;

wherein the wireless device is configured to receive a shared secret from the server upon determining that a shared secret does not exist with the server, by establishing a first secure tunnel with server using asymmetric encryption, receiving the shared secret via the first secure tunnel from the server, and tearing down the first secure tunnel after receiving the shared secret;

wherein the wireless device is configured to establish a subsequent[[,]] new secure tunnel between the wireless device and the server after the first secure tunnel has been torn down and upon determining the shared secret exists by using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret;

wherein the wireless device is configured to mutually authenticate with the server employing the subsequent[[,]] new secure tunnel; and

wherein the wireless device is configured to derive keying material that binds the subsequent new secure tunnel with all conversations inside the subsequent new secure tunnel.

25. (Canceled)

26. (Previously Presented) A wireless device according to claim 24, wherein the wireless device is further configured to establish a session key seed for deriving a master session key used for mutually authenticating the wireless device employing the secure tunnel.

27. (Currently amended) A method according to claim 1, further comprising establishing a plurality of subsequent[[,]] new secure tunnels between the peer and server using the shared secret.